I MANUALI OPERATIVI DEI CERTIFICATI

InfoCert S.p.A., in qualità di Ente Certificatore, ha pubblicato, per ogni tipologia di Certificato Digitale, un apposito Manuale Operativo e/o Certificate Policy in cui sono descritte dettagliatamente le caratteristiche tecniche dei certificati digitali, gli obblighi e le responsabilità delle parti, le leggi vigenti e le tariffe, le procedure (registrazione dei richiedenti, richiesta, emissione, revoca e sospensione), le informazioni relative alle misure di sicurezza ed il sistema di qualità adottato dal Certificatore. Tali Manuali, soggetti a revisioni ed a nuove versioni, legate all'evoluzione della tecnica e della normativa, devono essere letti attentamente dal richiedente, prima del rilascio dei certificati digitali in suo favore, nonché dagli utilizzatori degli stessi e sono reperibili sul sito www.firma.infocert.it. Si informa espressamente il richiedente che l'utilizzo di una firma digitale, per cui sia stato emesso un certificato di sottoscrizione, comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona. Per tale motivo il richiedente è obbligato ad osservare la massima diligenza nell'utilizzo, conservazione e protezione della chiave privata, del dispositivo di firma e del codice di attivazione ad esso associato (PIN). Lo stesso Utente Titolare è tenuto a proteggere la segretezza della chiave privata, non comunicando o divulgando a terzi il codice personale identificativo (PIN) di attivazione della stessa, provvedendo a digitarlo con modalità che non ne consentano la conoscenza da parte di altri soggetti e conservandolo in un luogo sicuro e diverso da quello in cui è custodito il dispositivo contenente la chiave. La chiave privata, per cui è stato rilasciato il certificato di sottoscrizione, è strettamente personale e non può essere per alcuna ragione ceduta o data in uso a terzi. Si informa che non esistono, alla data, accordi di certificazione (cross certification) in essere tra InfoCert ed altri Certificatori iscritti nell'elenco CNIPA: accordi successivi saranno resi pubblici sul sito **www.firma.infocert.it**.

Inoltre, secondo quanto stabilito dall'art. 32 del Codice Amministrazione Digitale, (D.L.vo 7 marzo 2005, n. 82, emendato dal D. Lgs. 4 aprile 2006, n. 159), il richiedente può ottenere tutte le informazioni, inerenti alla procedura di certificazione, ivi comprese le modalità di identificazione, registrazione e rilascio del dispositivo, attraverso la lettura dei capitoli 4 e 5 del Manuale Operativo di Sottoscrizione (ICERT-INDI-MO); non sono stabiliti particolari requisiti tecnici per accedere alla procedura. Ai fini dell'utilizzo del certificato digitale occorre, comunque, poter disporre della seguente dotazione hardware e software:

- Personal Computer con collegamento ad Internet e casella di posta elettronica;
- lettore di smart card (per certificati rilasciati su tale tipologia di dispositivi);
- software di firma digitale (sul sito **www.firma.infocert.it** si può scaricare, gratuitamente, l'ultima versione del software DiKe distribuito da InfoCert).

Si ricorda agli utenti della firma digitale di accertarsi che i sistemi informatici utilizzati siano adeguatamente protetti da antivirus o da altri programmi idonei ad evitare rischi di intrusione.

ISTRUZIONI PER L'UTILIZZO DEI CERTIFICATI DIGITALI

(rilasciati su dispositivi smart card o Business Key)

Ai fini dell'utilizzo dei certificati digitali occorre seguire le seguenti istruzioni:

1. la busta e il suo contenuto (CODICE di EMERGENZA o ERC, numero di dieci cifre, ex RRC) deve essere conservata con cura, per tutto il tempo di validità del certificato. E' essenziale per l'utilizzo dei certificati di firma digitale e per altre, eventuali operazioni future.
2. il numero stampato all'esterno della busta è esclusivamente un progressivo, da non utilizzare come PIN.
3. non divulgare assolutamente a persone diverse dal titolare i codici PIN , PUK ed ERC contenuti nella busta.
4. tre tentativi sono il numero massimo di prove per la digitazione corretta del PIN, superati i quali il dispositivo si blocca; per sbloccare il dispositivo utilizzare il PUK. Vedi istruzioni nel sito **www.firma.infocert.it**.
5. per sospendere un certificato digitale è necessario conoscere lo IUT (Identificativo Univoco del Titolare), inserito nel modulo di Richiesta di Registrazione e Certificazione. La funzione di sospensione è disponibile sul sito **www.firma.infocert.it**.
6. per accedere ai servizi online (es. Servizi CNS) effettuare l'installazione del software di autenticazione (vedi istruzioni nel sito **www.firma.infocert.it**).

Per dispositivi di firma con numero di serie 1203.., 14.., 15.., 16.., 0120..

7. il codice contenuto nella busta (di dieci cifre complessive) contiene le seguenti informazioni:

ERC (Emergency Request Code, ex RRC) è il numero completo di dieci cifre che deve essere utilizzato per l'autenticazione della richiesta di sospensione dei certificati digitali;
PIN (Personal Identication Number) iniziale è formato dalle ultime cinque cifre, da personalizzare come descritto in seguito; è associato alle funzionalità di firma digitale e consente l'accesso ai certificati digitali contenuti nel dispositivo;
PUK (Personal Unblock Key) è formato dalle ultime otto cifre, necessarie allo sblocco del dispositivo.

8. il titolare entrato in possesso del dispositivo deve, per ragioni di sicurezza, modificare il proprio PIN. Per istruzioni visitare il sito **www.firma.infocert.it .**

Per dispositivi Carta Nazionale dei Servizi (smart card o Business Key) serie 1204.., 1205, 7420.., 6090..

9. il codice contenuto nella busta (di dieci cifre complessive) contiene le seguenti informazioni:

ERC (Emergency Request Code, ex RRC) è il numero completo di dieci cifre da utilizzare per l'autenticazione della richiesta di sospensione dei certificati digitali;
PIN "CNS" (Personal Identification Number) iniziale è formato dalle ultime otto cifre e consente l'utilizzo del dispositivo;
PUK "CNS" (Personal Unblock Key) iniziale è formato dalle ultime otto cifre necessarie allo sblocco del PIN del dispositivo;
PIN "firma" iniziale è formato dalle ultime otto cifre e permette l'operazione di firma digitale (costituita dalla digitazione consecutiva del PIN CNS e del PIN firma);
PUK "firma" iniziale è formato dalle ultime otto cifre necessarie allo sblocco del PIN firma.

10. il Titolare, entrato in possesso del dispositivo, prima di eseguire qualsiasi operazione, deve attivarlo, utilizzando l'applicazione "DiKeUtil" (disponibile gratuitamente sul sito **www.firma.infocert.it**) o con la funzione "Gestione PIN" della Business Key; successivamente il titolare può decidere se modificare o meno i PIN

Per ulteriori informazioni o per risolvere eventuali problemi relativi all'attivazione del dispositivo e all'uso dei Certificati, si può consultare il sito **www.firma.infocert.it**

ISTRUZIONI PER L'UTILIZZO DEI CERTIFICATI DIGITALI

(rilasciati su dispositivi HSM per Firma Digitale Remota e Automatica)

Ai fini dell'utilizzo dei certificati digitali occorre seguire le seguenti istruzioni:

1. la busta ERC (anche se fornita in modalità elettronica) e il suo contenuto deve essere conservata con cura, per tutto il tempo di validità del Certificato. E' essenziale per l'utilizzo dei certificati di firma digitale e per altre, eventuali operazioni future.
2. il numero stampato all'esterno della busta fisica è esclusivamente un progressivo, da non utilizzare come PIN.
3. non divulgare assolutamente a persone diverse dal titolare i codici PIN , PUK ed ERC contenuti nella busta.
4. tre tentativi sono il numero massimo di prove per la digitazione corretta del PIN, superati i quali il certificato di firma digitale su dispositivo HSM si blocca per 10 (dieci) minuti; trascorso il tempo di blocco il certificato ritorna utilizzabile.
5. se il PIN viene dimenticato o smarrito il Certificato deve essere revocato e si deve richiedere l'emissione di un nuovo Certificato.
6. per sospendere o revocare un Certificato è necessario conoscere lo IUT (Identificativo Univoco del Titolare), inserito nel modulo di Richiesta di Registrazione e Certificazione e nella mail di avviso di avvenuta registrazione. La funzione di sospensione è disponibile sul sito **www.firma.infocert.it**.
7. per l'utilizzo del Certificato è necessario l'utilizzo contemporaneo della User ID, del codice temporaneo OTP e del PIN.
8. le istruzioni per l'utilizzo e la gestione del Certificato sono consegnate al Titolare via email al momento della richiesta di registrazione e possono essere consultate sul portale di gestione del Certificato all'indirizzo https://ncfr.infocert.it , per i certificati di firma remota, e https://ncfa.infocert.it , per i certificati di firma automatica.
9. Il codice PIN presente nella busta ERC deve essere cambiato al primo accesso al portale di gestione del certificato; successivamente il titolare può decidere se modificare o meno il PIN sempre utilizzando l'apposita funzione all'interno del portale di gestione del Certificato.
10. Il Certificato di Firma Digitale Remota è utilizzabile con il Software Dike per Windows e con l'Applicazione per iPhone e iPad scaricabili gratuitamente rispettivamente dal sito www.firma.infocert.it e dall'Apple Store; le istruzioni sull'utilizzo sono presenti nei manuali d'uso presenti all'interno dei software Dike e Dike Mobile (solo per iPhone e iPad).